Joint Interpretation Library

Composite product evaluation for Smart Cards and similar devices

Object: Define concept and methodology applicable to composite product evaluation.

Version 1.5.1
May 2018

This page is intentionally left blank

Table of contents

Figures

Tables

Appendices

1 Introduction

1.1 History

1 The Common Criteria (CC) is being widely used for smart card products security evaluation. Smart card evaluation showed very early a need for interpretation and supporting documents.

2 The initial reason was that a smart card is built up with a combination of two parts: a hardware integrated circuit (IC) part and a software part often developed by different actors with specific objectives.

3 Another reason is that the software part may be layered itself consisting of an "Operating System layer" with possibly integrated applicative functions and an "Application layer" on top of it that may contain different applications. All these software parts can be developed by different actors with specific objectives.

4 One objective was to independently perform one evaluation of a platform to address several applications and customers.

5 Another objective was to create one or several applications to load on one or several certified platforms.

6 The objective for Application Integration was to install one or several applications onto one already certified platform to reduce the evaluation effort keeping a high level of confidence.

7 To achieve these objectives, a transfer of knowledge and a reuse of evidence have been defined.

1.2 Definitions

8 The hardware part and associated libraries (if applicable) is evaluated independently as it can be used with many different software applications.

9 The software is embedded in the hardware and is built to operate with this hardware. The resulting product is the one which is used in the field (cellular phones, banking cards, health cards, identity, digital signature, e-pass, e-ticketing etc.) and on which customers/users need to gain confidence.

10 Software applications may be built to operate with the support of an OS. The OS provides a separation mechanism between itself and the software applications as well as services to the software applications.

11 Another specificity of the smart card type product is that the software part has to use, control, configure or activate the security mechanisms provided by the hardware. And the software applications may use, control, configure or activate the security mechanisms provided by the OS.

1.3 Composite product evaluation and ACO (CC V3)

12 Although the CC version 3 introduces the specific assurance class ACO for composition, this class is not suitable for usual smart card and similar devices evaluation.

13 ACO addresses a TOE composed of two certified TOEs: the Base TOE and the Dependent TOE (see Figure 1). The evaluation of the composed TOE consists in evaluating the interaction between both TOEs, reusing evaluation results of Base TOE and Dependent TOE.

14 The result of this evaluation is not an EAL level, but a CAP level which is not comparable to an EAL level. Furthermore, ACO class is applicable up to Extended-Basic assurance level, whereas smart cards especially in banking or signature type application require 'High Level' assurance.

Figure 1 - ACO composed TOE (package CAP)

15 For smart card and similar devices the composite product is the final product for which **an EAL level certification is required**. This allows a direct comparison with similar products certified after a single evaluation.

16 Considering smart card architecture, it is composed of a hardware platform typically an integrated circuit and embedded software layer on top of the hardware platform. The embedded software may be itself an Application or is composed itself of an "OS layer" with a further "Application layer" on top of the „OS layer"". The hardware and maybe the "OS layer" together may form a Platform with an Application on top of it. In the **Composite TOE** evaluation, the Platform is certified, the Application is evaluated and the results of the Platform Certification are reused. See for **Figure 2** security certification of the entire Composite TOE.

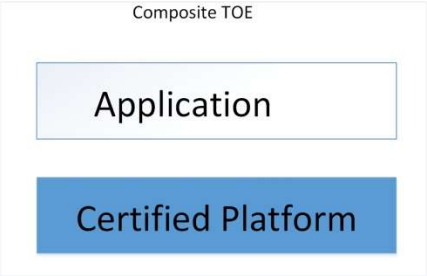


Figure 2 - Composite product evaluation (current approach)

17 The hardware platform properties related to security and security functionality are provided in the security target. The platform provides mechanisms to protect the composite product assets, but the composite product behaviour depends widely on the software application having to use, to configure and activate these security mechanisms.

18 The OS platform offers security services and provides mechanisms to protect the composite product assets. The composite product behaviour depends widely on the software application having to use the security services and to use, to configure and activate these services. Therefore, the platform evaluation results provide security recommendations and conditions formulated in the platform user guidance for the software application implementation.

19 The composite product evaluator shall examine amongst other that the combination of application and platform does not lead to any exploitable vulnerability. The smart card composite evaluation methodology defines precise work units with clear statement on the information needed from the platform developer and provides an agreed "framework" for information transfer from platform to composite product evaluator.

20 The information required is already available from the platform evaluation tasks and no additional work is required from platform developer.

- There is no need for details on the platform development class ADV.
- The user guidance (AGD) of the platform is considered early in the development of the composite product and provides all interfaces information needed.
- The development and the evaluation of the composite TOE rely on the proper implementation of the evaluated interfaces of the platform
- The proper use of all relevant interfaces between platform and application is in the scope of the composite product evaluation..
- Test (ATE) and vulnerability assessment (AVA) are performed on the composite product taking advantage of platform evaluation results.

21 The concept of the Composite TOE evaluation does not limit the composite evaluation in EAL and resistance against attacks, i.e. up to 'high', whereas Composed TOE (CAP package) is limited by resistance against attacks 'extended-basic'.

1.4 Objective and scope

22 The objective of this document is to precisely define tasks for the different parties involved in the Composite TOE evaluation.

23 The aim is not to define an additional assurance class, but to define refinements to the existing assurance requirements for a composite product evaluation.

24 This document addresses TOEs that are of the type belonging to the technical domain "**Smartcards and Similar Devices**". However, this document is not restricted to smart cards and similar devices only and can be applied in principle (possibly with adequate adaptations, as far as necessary) for any other secure IT product where an independently evaluated component is part of a final composite product to be evaluated.

25 The **smart cards and similar devices technical** domain is defined as: related to smart cards and similar devices where significant portions of the required security functionality depend upon hardware features at a chip level (for example smart card hardware/ICs, smart card composite products, TPMs (Trusted Platform Modules) used in trusted computing, digital tachograph cards, etc.) (source of definition: http//:www.sogis.eu).

2 Definitions / Terminology

2.1 Definitions

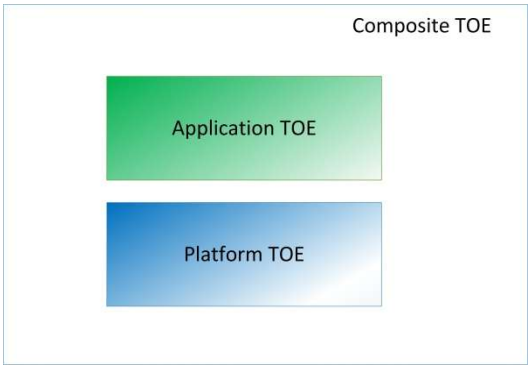


Figure 3 – Composite Product

26 The *Composite TOE* is a TOE that is composed of a superposition of 2 layers as depicted in **Figure 3**, the initial layer (identified as the 'Platform') and the supplementary layer (the 'Application').

- The initial layer is the underlying layer that could be either a single product, or a composite product. We consider that this layer has been already certified.
- The supplementary layer is dependent on the platform. This layer is subject to the composite evaluation.

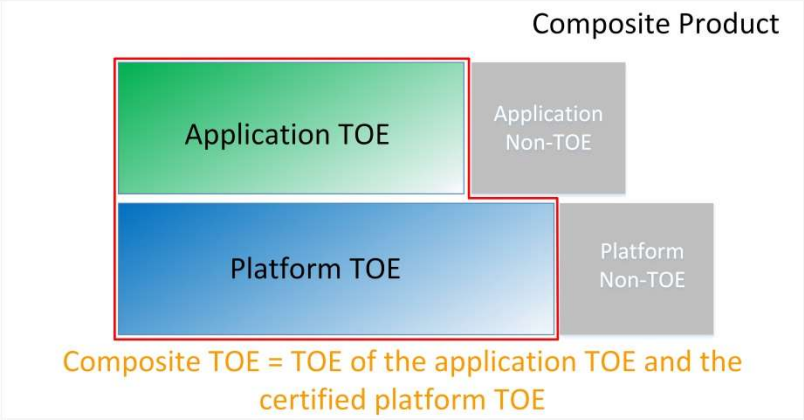


Figure 4 – Composite TOE

The *composite TOE* is a composition between the platform and the application, and is composed of the 'platform TOE' and the 'application TOE' as marked in the red box in **Figure 4**, with the following restrictions:

The application TOE cannot rely on platform functionalities that are outside the platform TOE, in the Non-TOE parts. This is depicted in grey layer 'Non-(platform) TOE' in **Figure 4**

- The composite TOE is composed with a superset of the entire application TOE, and a superset of the minimum platform TOE functionalities required for the correct execution of the composite product.
- The non-TOE subset of the application can use platform TOE functionalities. As usual, the composite evaluation needs to determine that this non-TOE application part is non-interfering with the application TOE – neither directly nor through the usage of the platform functionalities.

27 Exemplifying we can mention an operating system ('application') running on a hardware platform ('underlying platform') or a Java Card™ applet ('application') running on a Java Card runtime environment ('platform').

28 Several composition steps can follow each other i.e. a composite product may rely on a platform which is itself a composite product. For such compositions with a previously composed product the same rules apply.

29 These definitions comply with ACO class definitions where:

- A platform is the base component,
- An application is the dependent component.

2.2 Roles

30 The following roles shall be considered in the composite evaluation activities:

- **Platform Developer**: Entity developing the platform; it might also be the sponsor of the platform evaluation.
- **Platform Evaluator**: Entity performing the platform evaluation.
- **Platform Certification Body**: Entity performing the platform certification, defined in CC V3 terminology as evaluation authority.
- **Application Developer**: Entity developing the application running on the platform.
- **Composite Product Integrator**: Entity installing the applications on the platform.
- **Composite Product Evaluator**: Entity performing the composite product evaluation.

- **Composite Product Certification Body**: Entity performing the composite product certification defined in CC V3 terminology as evaluation authority.

- **Composite Product Evaluation Sponsor**: Entity in charge of contracting the composite product evaluation.

31 Each evaluation shall associate particular organizations or persons to these generic roles.

32 In order to illustrate the role of the **Composite Product Integrator** let us exemplify:

- Native Smart cards: The 'underlying platform' is an integrated circuit and the **Platform Developer** is the integrated circuit (chip) manufacturer; the 'application' is a card operating system and its application(s) and the **Application Developer** is the developer of the smart card software and the application(s). In this case, the role of the Composite Product Integrator is played by (i) the chip manufacturer embedding the core of the operating system into the ROM of the chip, then by (ii) the card manufacturer usually loading some parts of the operating system and the applications into NV-Memories (EEPROM and/or Flash) of the chip.

- Java Card technology-enabled devices: The 'underlying platform' is the Java Card runtime Environment (Java Card RE) on chip and the **Platform Developer** is the card manufacturer/issuer; the 'application' is the Java Card applet and may be developed by the **Application Developer**. In this case, another role is the **Composite Product Integrator** who may be played by the domain/application service provider or by a trust centre loading the applet and often personalizing the card electronically.

3 Composite evaluation concept

3.1 What are the issues?

33 The assets to be protected are the final composite product assets defined in the composite product Security Target.

34 The security mechanisms involved in the protection of these assets are those provided by the platform and by the application itself.

35 Some of the security mechanisms and security services provided by the platform may require configuration, programming or activation by the application.

36 Therefore the **Application Developer** needs all the information (in form of a guidance or user's manual) related to the platform security mechanisms and security services the application has to manage.

37 Furthermore he needs the platform security target in order to build the composite product security target and to ensure consistency of security definition between platform and application development. Evaluation is performed and validated on the final composite product.

38 If the Platform and the Application parts are combined in a composite product the **Composite Product Evaluator** has to examine, that the level of security required by the Security Target is achieved. Therefore the **Composite Product Evaluator** has to execute the evaluation tasks needed with respect to the Security Target of the final composite product and to provide the related ETR. In this perspective, the **Composite Product Evaluator** should reuse the platform's evaluation and certification result thus saving cost and time.

3.2 What information is needed?

39 The **Composite Product Evaluator** does not need all platform evaluation results. The security certificate and the certification report ensure that the platform has been evaluated according to the Common Criteria. The **Composite Product Evaluator** will need complementary information on the assurance measures where platform and application development interfere. To check that the application meets the security requirements of the platform usage, the **Composite Product Evaluator** will need the same level of knowledge about the platform as the **Application Developer.** In addition to the standard amount of evaluation contributions according to the assurance package chosen for the composite evaluation (e.g. an EAL level) evaluation, the following is needed (see section 4.7 'Deliveries' for further details):

- All the information delivered from the **Platform Developer** to the **Composite Product Integrator**,
- All the information delivered from the **Platform Developer** to the **Application Developer**,

- ETR for composite evaluation prepared by the **Platform Evaluator**, see chapter 5 'ETR for composite evaluation' (including information about vulnerability analysis and penetration testing),
- Information on compliance of the Security Targets and the designs of the platform and the application prepared by the **Application Developer**,
- Information on compliance of the delivery procedures of the **Platform** and **Application Developers** with the acceptance procedure of the **Composite Product Integrator**, and
- Information on integration of both parts using their correct certified versions and the correct configuration parameters. This information shall be prepared by the **Composite Product Integrator**; it also implies assurance that the application is correctly managed by the **Platform Developer** (e.g. in the case of smart card where ROM code is supplied for masking on the platform).

40 **Composite Product Certification Body** will need the same amount of information as the **Composite Product Evaluator**.

3.3 Case of composite product change

41 In case of composite product changes due to a minor change of the platform or the application or both, please refer to [CC AC].

42 If a change comes from the platform, the assessment of the change for the platform is given by the **Platform Certification Body**. On this basis, the assessment of the change for the composite product is given by the **Composite Product Certification Body**.

43 If a change comes from the application, the assessment of the change for the composite product is given by the **Composite Product Certification Body**.

3.4 Specific case when the application is already certified

44 In the case where both platform and application have already been certified, a partial evaluation work may be performed regarding the results already obtained from previous application evaluation. Nevertheless, the composite evaluation tasks as defined in this document are still required.

4 Composite evaluation activities description

45 The current approach can be applied independent of the evaluation assurance level (EAL) for the composite product aimed. Where some evaluation activities are not applicable due to the EAL chosen, they are also not expected to be applied.

46 For the following paragraphs, we assume that the level of assurance of the platform is equivalent or higher compared to the composite product evaluation level.

47 Other cases must be discussed within the schemes.

48 The composite-specific developer and evaluator action elements as well as the evaluator actions (work units) belonging to the composition activities are defined as the refinements for composite evaluation, see Appendix 1: Composite-specific requirements.

4.1 Evaluation of the composite product Security Target

49 A Security Target for the composite product has to be written and evaluated.

50 The **Composite Product Evaluator** has to examine that the Security Target of the composite product[1] does not contradict the Security Target of the underlying platform[2]. In particular, it means that the **Composite Product Evaluator** has to examine the Composite- and the Platform- Security Target for any conflicting assumptions, compatibility of security objectives, security requirements and security functionality needed by the application.

[R1] This task can be reduced, if some matching has been checked for Protection Profiles claimed by each Security Target.

[R2] The **Composite Product Evaluation Sponsor** must ensure that the security target of the platform is available to the **Application Developer**, to the **Composite Product Evaluator** and to the **Composite Product Certification Body**. The information available in public version of the security target may not be sufficient.

4.2 Integration of the application in the configuration management system

[R3] The **Composite Product Evaluator** shall verify that the evaluated version of the application has been installed onto / embedded into the evaluated version of the underlying platform.

[1] denoted by Composite-ST in the following

[2] denoted by Platform-ST in the following

[R4] The **Composite Product Evaluation Sponsor** must ensure that appropriate evidence generated by the **Composite Product Integrator** is available to the **Composite Product Evaluator**. This evidence may include, amongst other, the configuration list of the **Platform Developer** provided within its acknowledgement statement.

4.3 Compatibility check for delivery and acceptance procedures

[R5] The **Composite Product Evaluator** shall verify that delivery procedures of the **Application** and **Platform Developers** are compatible with the acceptance procedure used by the **Composite Product Integrator**.

[R6] The **Composite Product Evaluator** shall verify that all configuration parameters prescribed by the **Application** and **Platform Developers** (e.g. pre-personalization data, pre-personalisation scripts) are used by the **Composite Product Integrator**.

[R7] The **Composite Product Evaluation Sponsor** must ensure that appropriate evidence generated by the **Composite Product Integrator** is available to the **Composite Product Evaluator**. This evidence may include, amongst other, the

- Element of evidence for the application reception, acceptance and parameterisation by the **Platform Developer** (in form of acknowledgement statement).

4.4 Compliance of designs

[R8] The **Composite Product Evaluator** shall verify that stipulations for the **Application Developer** imposed by the **Platform Developer** in its certified user guidance and referenced in the platform certification report are fulfilled by the composite product, i.e. have been taken into account by the **Application Developer**.

[R9] The **Composite Product Evaluation Sponsor** must ensure that the following are made available to the **Composite Product Evaluator**:

- The platform-related user guidance,
- ETR for Composition prepared by the **Platform Evaluator**, see chapter 5 ‘ETR for composite evaluation’,
- The Certification Report for the platform prepared by the **Platform Certification Body**,
- A rationale for secure composite product implementation including evidence prepared by the **Application Developer**.

4.5 Composite product functional testing

[R10] Some application functionality testing can only be performed on emulators, before its embedding/integration onto the platform, as effectiveness of this testing (pass/fail) may not be visible using the interfaces of the composite product. Nevertheless, functional testing of the composite product shall be performed also on composite product samples according to description of the security functions of the Composite TOE and using the standard approach as required by the relevant assurance class. No additional developer's action is required here.

[R11] Since the amount, the coverage and the depth of the functional tests of the platform have already been validated by the platform certificate, it is not necessary to re-perform these tasks in the composite evaluation. Please note that ETR for Composition (see chapter 5 'ETR for composite evaluation') does not provide any information on functional testing for the platform.

[R12] The **Composite Product Evaluation Sponsor** must ensure that the following is available to the **Composite Product Evaluator**:

- Composite product samples suitable for testing.

4.6 Composite product vulnerability analysis

[R13] The **Composite Product Evaluator** shall perform a vulnerability analysis for the composite product using, amongst other, the results of the platform evaluation and certification. This vulnerability analysis shall be confirmed by penetration testing.

[R14] The **Composite Product Evaluator** has to check that the confidentiality protection of the embedded software in memory of the platform is consistent with the confidentiality level claimed by the **Application Developer** for ALC_DVS.

[R15] In special cases, the vulnerability analysis and the definition of attacks might be difficult, need considerable time and require extensive pre-testing, if only documentation is available. The platform may also be used in a way that was not foreseen by the **Platform Developer** and **Platform Evaluator**, or the **Application Developer** may not have followed the stipulations provided with the platform certification. Different possibilities exist to shorten composite vulnerability analysis in such cases:

- The **Composite Product Evaluator** can consult the **Platform Evaluator** and draw on his experience gained during the platform evaluation.

- Separation of vulnerabilities of application and platform with the use of "open samples" ("open samples" are samples of the platform on which the **Composite Product Evaluator** can load software on his own discretion). The intention is to use test software without the application countermeasures without deactivating any platform inherent

countermeasure. The aim is clearly not to repeat the platform evaluation. (See the mandatory [JIL AP] for further details).

[R16] The **Composite Product Evaluation Sponsor** must ensure that the following are made available to the **Composite Product Evaluator**:

- *The ETR for Composition* (ETR_COMP) prepared by the **Platform Evaluator**, see chapter 5 'ETR for composite evaluation' below, and
- The Certification Report for the platform prepared by the **Platform Certification Body**.

4.7 Deliveries

51 The tables below summarize the documentation deliveries that are exchanged between parties to enable the composite evaluation activities as defined in the previous paragraphs.

52 The **Composite Product Evaluation Sponsor** is in charge of the initialization of the process.

53 The **Composite Product Evaluation Sponsor** is responsible for maintaining or creating any **Non-Disclosure Agreement** (NDA) that would be necessary between all the parties involved in the composition activities.

54 The **Non-Disclosure Agreement** should be established according to the sensitivity and ownership of the information to be exchanged

##	Document / Contribution	Description
1	Platform Security Target	Security Target of the platform as referenced in the platform certification report.
2	Platform open samples for testing	Platform samples as defined in [JIL AP] Chapter 3.8.
3	Platform user guidance	It encompasses all platform user guidance and manuals needed for the **Application Developer** and the **Composite Product Integrator** being referenced in the platform certification report.
4	Platform ETR_COMP	ETR for composition as defined in chapter 5 and referenced in the platform certification report.
5	Platform certification report	Platform certification report issued by authorized **Platform Certification Bod**y.
6	Design compliance evidence	It enfolds evidence elements on how the requirements on the application design, imposed by the platform's guidance and certification report, are fulfilled in the composite product. If such a requirement was not followed, a rationale

##	Document / Contribution	Description
		that the chosen composite product implementation is still secure shall be given here.
7	Composite configuration evidence	It comprises (i) Identification elements of the composite product - proving that the correct, certified version of the platform is used in the composite product, - proving that the correct, evaluated version of the application has been integrated; and (ii) Evidence elements that security measures prescribed by the **Platform** and **Application Developers** are actually being applied by the **Composite Product Integrator**.
8	Delivery and acceptance procedures evidence	Evidence elements how the delivery procedures of the **Platform** and **Application Developers** are compatible with the acceptance procedure of the **Composite Product Integrator**

Table 1 - Definition of composition documents

55 The following table shows which documents/contributions of Table 1 shall be provided to which actor within the composite evaluation process:

		Actors				
##	**Documents/contributions having to be provided to**	**Composite product evaluation Sponsor**	**Composite product integrator**	**Applica-tion developer**	**Composite product Evaluator**	**Composite product Certifica-tion Body**
1	Platform Security Target	No	No	Yes	Yes	Yes
2	Platform open samples[3]	No	No	No	Yes	No
3	Platform user guidance	No	Yes	Yes	Yes	Yes
4	Platform ETR_COMP	No	No	No	Yes	Yes
5	Platform certification report	Yes	Yes	Yes	Yes	Yes
6	Design compliance evidence	No	No	No	Yes	Yes

[3] Only if requested by composite product evaluator as defined in [CC-AP]

		Actors				
##	**Documents/contributions having to be provided to**	**Composite product evaluation Sponsor**	**Composite product integrator**	**Applica-tion developer**	**Composite product Evaluator**	**Composite product Certifica-tion Body**
7	Composite configuration evidence	No	No	No	Yes	Yes
8	Delivery and acceptance procedures evidence	No	No	No	Yes	Yes

Table 2 - Main Deliveries between actors

56 The next table shows some example of Composite TOE use cases with definition of the components and the roles.

	Composite TOE example		
Components & roles definitions	**Smartcard –I** The Composite TOE is built of - a Security IC with an application code loaded in ROM (Masking operation) and application data loaded in EEPROM.	**Smartcard –II** The Composite TOE is built of - a Security IC without ROM, but offering Flash technology and Flash loader - an application code and data loaded into the flash by a smart Card manufacturer	**Java Card** The Composite TOE is built of - a Java Card Platform - a Java card application: the applet
The **Platform** is	The Security IC	The Security IC with the Flash memory and the Flash Loader	The Java Card Platform including Card Manager with Applet loader facility
The **Application** is	The Operating System code plus additional data files	The Operating System code, Flash memory initialization data and application data	The Applet
The **Platform Developer** is	The Security IC Manufacturer: - Develops and manufactures the Security IC	The Security IC Manufacturer: - Develops, manufactures and delivers the Security IC with Flash technology to the Composite Product Integrator	The Java Card Platform developer: - Develops the Java Card with applet loading mechanism to the Composite Product Integrator.
The **Application Developer** is	The Smartcard Software developer: - Develops the application; - Provides the application to Composite product integrator	The Smartcard Software developer: - Develops the application; - Delivers the application to the Composite Product Integrator	The Applet developer: - Develops the applet; - Delivers the applet to the Composite Product Integrator

	Composite TOE example		
The **Composite Product Integrator** is	The Security IC Manufacturer: - is in charge of OS masking in ROM and of loading Application data in EEPROM; - Delivers the Composite TOE to be evaluated	The Card Manufacturer: - is in charge of loading the application into the flash using Security IC flash loader; - Delivers the Composite TOE to be evaluated	The Card Issuer: - Loads the applet on the Java Card platform using applet loading mechanism; - Delivers the Composite TOE to be evaluated

Table 3 - Example of composite TOE use cases

5 ETR for composite evaluation

5.1 Objective of the document

57 A standard Evaluation Technical Report (ETR) contains proprietary information that cannot be made public. The *ETR for composite evaluation* (ETR_COMP) document is compiled from the ETR in order to provide sufficient information for composite product evaluation with a certified platform. The information that is presented in the ETR_COMP document shall be a subset of the information presented in the full ETR. It should enable the **Composite Product Evaluator** and the respective **Certification Body** to understand the considered attack paths, the performed tests and the effectiveness of countermeasures implemented by the platform.

58 A template for an **ETR_COMP** document is given in Appendix 2: ETR for composite evaluation template.

5.2 Generic rules:

[R17] The *ETR for composite evaluation* should be produced by the **Platform Evaluator** based on the platform evaluation results. This task should be considered when determining the evaluation work program to reduce additional cost and effort.

[R18] The content of ETR_COMP has to strike the right balance between protecting platform developer's and/or **Platform Evaluator's** proprietary information and providing sufficient information for the **Composite Product Evaluator** and the respective **Certification Body**, cf. Table 2 above.

[R19] ETR_COMP shall not include information affecting national security.

[R20] The information provided must be approved by all parties involved in the platform evaluation (i.e. the Evaluator, the Certification Body, the developer and sponsor of the evaluation). The platform Certification Body shall validate its consistency with the original ETR. The platform certification report shall reference the *ETR for composite evaluation*.

[R21] If the current ETR_COMP itself relies on a composite evaluation, and if there is direct interface with the previous platform, the reference to this previous composite evaluation ETR_COMP must be supplied.

[R22] The ETR_COMP is not meant to include copies of information from other available platform evidence, as the Security Target and Guidance. However, the composite evaluation is much supported by references to the relevant sections.

5.3 Exchange of the ETR for Composition

59 An ETR_COMP contains intellectual property of the **Platform Developer** as well as of the **Platform Evaluator**, and also **the Platform Certification Body** has a role in its content. At the minimum the document should be considered restricted. The ETR_COMP document is created and maintained by the **Platform Evaluator**. However, at a given certification the Platform developer is the point of contact for the **Application Developer**.

60 The application developer will contact the **Platform Developer** for delivery of the ETR_COMP to the point of contact at the **Composite Product Evaluator**. The **Platform Developer** will check its confidentiality management rules (existence of relevant NDA with Lab and CB, etc.) whether delivery is possible. If necessary the platform developer will contact the **Platform Certification Body** about the intent of the delivery of the ETR_COMP.

61 Next the **Platform Developer** will contact the **Platform Evaluator** to request the delivery (using a secure method and only marked versions will be distributed) of the ETR_COMP to the given contact point of the **Composite Product Evaluator**. If the OK is granted, either the **Platform Evaluator** or the **Platform Developer** will send the ETR_COMP to the **Composite Product Evaluator** depending on the agreements between these two parities.

62 Depending on (contractual) agreement between the **Platform Developer** and **Platform Evaluator**, there may be deviations from the described procedure of delivery of the ETR_COMP to the **Composite Product Evaluator**.

63 If necessary the **Platform Evaluator** and the **Composite Product Evaluator** will exchange more detailed information. This is always under control of the **Platform Developer**. In case of clarification the **Platform Evaluator** and the **Composite Product Evaluator** will be the main parties. If an additional assurance statement is required then also the **Platform certification body** will be involved in the exchange.

5.4 Content of the ETR for composite evaluation

[R23] The information required is focused on:

1. Formal information about the platform like its exact identification, reference to the certification report etc.
2. Information about the Platform design.
3. Information about the evaluated configuration of the Platform.
4. Information on delivery procedures, involved sites and data exchange.
5. Information about penetration testing of the Platform including the considered attack paths and summary of test results.

6. Information about penetration testing of the supporting functions in the platform

7. Observations and recommendations for users.

5.4.1 Formal information

[R24] This section of ETR_COMP shall provide formal information on the platform evaluation as:

- product identification,
- sponsor and developer identities,
- identities of the evaluation facility and the certification body,
- assurance level of the evaluation,
- formal evaluation and certification results like pass/fail,
- references to the ETR.

5.4.2 Platform design

[R25] This section of ETR_COMP shall provide a high-level description of the IT product and its major components based on the deliverables required by the assurance class ADV of the Common Criteria. The intent of this section is to characterize the degree of architectural separation of the major components and to show possible technical dependencies between the platform and an application using the platform (e.g. dependencies between HW platform and SW application). This shall include an outline of security mechanisms of the platform covered by the platform evaluation.

5.4.3 Evaluated configuration

[R26] This section of ETR_COMP shall provide information about the evaluated configuration of the Platform based on the developer's configuration list or relevant parts as needed or on a case by case basis. The platform must unambiguously be identifiable and this identification shall be commensurate with the evaluated configuration as stated in the platform certification report.

[R27] If applicable, generation and installation parameter settings being security relevant for the Platform should be explained and their effect on the defence against attacks is outlined (e.g. key length, counters limits). This includes methods for the application developer and evaluator to verify the values of these settings, in order to verify that the expected evaluated configuration is used.

[R28] This evidence may include TOE installation, generation and start-up procedures as outlined in AGD_PRE to enforce that the platform is configured in a secure manner.

5.4.4 Delivery procedures, sites and data exchange

[R29] For supporting composite evaluation, evaluation evidence can be necessary for delivery of the platform, and acceptance procedures of the application and related data to be integrated during development and production. Therefore, evaluation evidence about AGD_PRE[4] and ALC_DEL + AGD_PRE[5] might be relevant.

[R30] The ETR_COMP shall provide an overview of the sites involved in the development and production of the platform, including the role of each site and the date of latest site visit.

[R31] For the composite evaluation, of an OS on an IC the description of phase 1 and 4 are needed and will be detailed in this document. The delivery of the IC dedicated software and guidance to the application developer should also be considered. In addition details on the fab-key protection mechanism should be identified.

For an IC as per the evaluation guide “The application of CC to IC” (cf. [CC IC]), the deliveries under consideration are:

1. The delivery of the embedded application code to the microcontroller manufacturer, (in case of Flash products this may be replaced by the delivery of a key from the microcontroller manufacturer to the developer of the Security IC Embedded Software)
2. The delivery of the microcontroller to the entity in charge of the next step (testing, embedding into micro-module, card manufacturing).

For an OS the deliveries under consideration are:

1. The delivery of the embedded application code to the manufacturer (if the code will be embedded in ROM) or product integrator (if the code will be embedded in EEPROM or Flash).
2. The delivery of the smart card/platform (IC with embedded OS) to the in charge of the next step (product integrator, personaliser, etc.)
3. The delivery of security guidance

[4] [1.2C]

[5] [1.1C]

4. The exchange of key-material for access to the smart card/platform (IC with embedded OS).

5.4.5 Penetration Testing

[R32] This section of ETR_COMP shall provide information about the independent vulnerability analysis performed by the **Platform Evaluator** with the attack scenarios having been considered, the penetration testing having been performed and the reference to the corresponding rating (quotation) of the attack potential (following the [JIL AP] valid at the time of the platform certification).

[R33] Information about penetration testing results should include:

- details necessary for understanding the attack scenarios/paths
- the assessments of penetration results as well as a summary showing that all attack methods as outlined in [JIL AP] were addressed during the vulnerability analysis.

If a potential vulnerability has to be resolved by adhering to guidance this must be clear from the summary including a reference to a specific section in guidance or if possible a guidance element.

[R34] The attack scenario descriptions should provide sufficient details to support the **Composite Product Evaluator** to reproduce attacks, which require additional countermeasures in the Composite TOE.

[R35] In accordance with the requirements of CEM[6], this information is available within the ETR. So it can be compiled for ETR_COMP.

[R36] This section shall also mention the rating of access to 'open samples' (i.e. public/restricted/sensitive/critical). The use of 'open samples' shall be considered in the assessment of the attack path. Please note that 'open samples' are evaluation tools, but do not represent a TOE.

5.4.6 Observations and recommendations

[R37] The evaluated user guidance documentation shall contain all information required to use the TOE in a secure way as defined in the platform security target including recommendations on how to avoid residual vulnerabilities and unexpected behaviour. The recommendations and the user guidance documentation shall be consistent. The **Platform Evaluator** shall verify that the ETR for Composition only contains recommendations on the secure use that are also addressed as requirements in the user guidance**.** The user

[6] Evaluation Methodology; depends on the version of CC chosen

guidance requirements must be specific enabling the A**pplication Developer** to perform design compliance analysis

[R38] However, in specific cases detailed information might be required in addition to the guidance documents such as:

- Observations on the evaluation results (e.g. specific TOE configuration for the evaluation),
- Recommendations/stipulations for the **Composite Product Evaluator**: specific information on use of the evaluation results (e.g. about specific testing necessary during a composition evaluation).

Any such observation or recommendation/stipulation may come from the **Platform Evaluator** and the **Platform Certification Body**.

6 Evaluation/Certification reports and Platform certificate validity

[R39] Results of a composite evaluation shall be provided to the **Composite Product Certification Body** in form of an Evaluation Technical Report for the composite product. This Composite Product ETR shall contain, amongst others, the final overall verdict for the composite evaluation based on the partial verdicts for each assurance component being in scope of the current composite evaluation. There shall be a reference to this CC supporting document in the Composite Product ETR and the Composite Product Certification Report.

[R40] As the composite product certificate covers also the platform, the composite product certificate validity is linked to the validity of the platform certificate.

[R41] The **Composite Product Certification Body** needs an up-to-date certificate or an assessment from the **Platform Certification Body** on the status of the platform certificate in question.

[R42] As a general rule the **Composite Product Certification Body** will ask for a reassessment of the platform if the date of the platform's ETR for Composition is more than one and a half year before the submission of the report containing the full results of the composition penetration tests. This reassessment consists of either a re-evaluation of the platform focussing on a renewal of the vulnerability analysis (surveillance task) or alternatively, a confirmation statement of the **Platform Certification Body** may be requested.

[R43] Note that in the case the entire composite product is set up as a chain of composite products constructed on top of each other (e.g. the platform itself is already a composite product) the maximum validity period of 18 months is related to the eldest ETR for Composition used in this chain of composite products. In addition, dependencies from a lower level ETR for Composition to a higher level ETR for Composition need to be considered when reusing the results in the composite evaluation on top.

[R44] Note also that if the platform's ETR for Composition was issued less than a year and a half ago before submission of the related composite evaluation tasks, but there was a major change in the state of the art in performing relevant attacks on the platform (e.g. a major change in the "Application of Attack Potential to Smart Cards" document [JIL AP] or a major change in attack methods or attack ratings) then the **Composite Product Certification Body** has the right to require a reassessment focusing on the new attack method.

[R45] Validity and relevance of the platform certificate for the current composite product certification shall be acknowledged by the **Composite Product Certification Body** and includes the determination of equivalence of single

assurance components (and, hence, of assurance levels) belonging to different CC versions, if the platform certification was according to another CC version than the current composite certification is. Such equivalence shall be established / acknowledged by the **Composite Product Certification Body**.

[R46] The **Composite Product Certification Body** can issue a security certificate for the composite product, if

- the verdicts for the Composite Product ETR is PASS and
- validity and topicality of the platform certificate for the current composite product is acknowledged by the **Composite Product Certification Body**.

[R47] Note that, if the **Composite Product Evaluator** detects some failures resulting from Platform testing (e.g. vulnerabilities due to improved attack methods or techniques), the results shall be communicated to the **Composite Product Certification Body**. The **Composite Product Certification Body** shall then take appropriate steps together with the **Platform Certification Body**, e.g. to invoke a re-assessment or re-certification of the platform TOE.

[R48] The **Platform Certification Body** shall verify that the recommendations in the ETR for composition of the platform are consistent with the requirements provided in the platform user guidance before issuing the certification report. When inconsistencies are detected the **Platform Certification Body** has the freedom to add missing information for the **Application Developer** in the certification report.

7 References

7.1 CC V3 documents

[CC] CCMB-2012-09-001 : Part 1 Introduction and general model, Version 3.1, Revision 5, April 2017

CCMB-2012-09-002 : Part 2 Security Functional components, Version 3.1, Revision 5, April 2017

CCMB-2012-09-003 : Part 3 Security Assurance Components, Version 3.1, Revision 5, April 2017

[CEM] CCMB-2012-09-004 : Evaluation Methodology, Version 3.1, Revision 5, April 2017

7.2 Supporting documents

[JIL AP] Joint Interpretation Library Application of Attack Potential to Smart Cards latest approved version

[CC AC] Assurance continuity: CCRA requirements

latest approved version

Appendix 1: Composite-specific requirements

In the following, the Composite-specific developer and evaluator action elements as well as the evaluator actions (*work units*) belonging to the composition activities (cf. chapter 4 above) are defined. They require the evidence elements as listed in section 4.7.

These refinements to the assurance requirements aim to give the **Composite Product Evaluator** and **Application developer** a precise guidance on which relevant aspects have to be described and assessed in the context of a composite evaluation and the tasks to be performed.

It allows the **Composite Product Certification Body** to check using the composite product ETR that the required (mandatory) tasks have properly been performed.

All composite-specific evaluator actions have to be documented according to the scheme rules and finalised by one of the verdicts PASS, FAIL or INCONCLUSIVE. As these actions are refinements of the traditional actions focused on the composition activities, these verdicts have to be integrated to the overall verdict.

This approach can be applied independently of the aimed evaluation assurance level (EAL) for the composite product. Where some evaluation activities are not applicable due to the EAL chosen, the related composite-specific tasks are also not expected to be applied.

For convenience of composite-specific activities and associated work units identification, each refinement is named as *_COMP, where * is the name of the assurance class it is related to.

Appendix 1.1: Composite-specific tasks for a composite evaluation in CC V3.1

Consistency of composite product Security Target (ASE_COMP)

The composite-specific work units defined in this chapter are intended to be integrated as refinements to the evaluation activities of the ASE class listed in the following table. The other activities of ASE class do not require composite-specific work units.

CC assurance family	Evaluation activity	Evaluation work unit	Composite-specific work unit
ASE_OBJ	ASE_OBJ.2.1C	ASE_OBJ.2-1	ASE_COMP.1-5
	ASE_OBJ.2.1C	ASE_OBJ.2-1	ASE_COMP.1-6
	ASE_OBJ.2.3C	ASE_OBJ.2-3	ASE_COMP.1-6
ASE_REQ	ASE_REQ.1.6C	ASE_REQ.1-10	ASE_COMP.1-1
	ASE_REQ.2.9C.	ASE_REQ.2-13	ASE_COMP.1-1
	ASE_REQ.1.6C	ASE_REQ.1-10	ASE_COMP.1-2
	ASE_REQ.2.9C.	ASE_REQ.2-13	ASE_COMP.1-2
	ASE_REQ.2.8C	ASE_REQ.2-12	ASE_COMP.1-3
	ASE_REQ.2.3C	ASE_REQ.2-4	ASE_COMP.1-4

ASE_COMP.1 Consistency of Security Target

Objectives

1 The aim of this activity is to determine whether the Security Target of the composite product[7] does not contradict the Security Target of the underlying platform[8].

Application notes

2 These application notes aid the developer to create as well as the evaluator to analyse a composite Security Target and describe a general methodology for it. For detailed information / guidance please refer to the single work units below.

3 In order to create a composite Security Target the developer should perform the following steps:

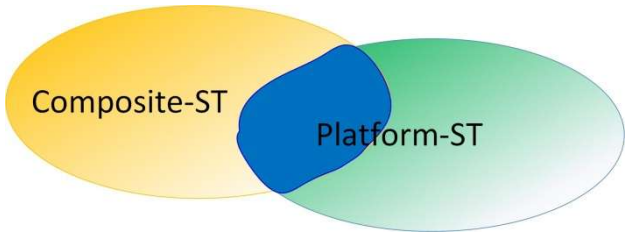
4 Step 1: The developer formulates a preliminary Security Target for the composite product (the Composite-ST) using the

[7] denoted by Composite-ST in the following

[8] denoted by Platform-ST in the following. Generally, a Security Target expresses a security policy for the TOE defined.

standard code of practice. The Composite-ST can be formulated independently of the Security Target of the underlying platform (Platform-ST) – at least as long as there are no formal PP conformance claims.

5 Step 2: The developer determines the overlap between Platform-ST and Composite-ST through analysing and comparing their TOE Security Functionality (TSF) [9][10]:



6 Step 3: The developer determines under which conditions he can trust in and rely on the Platform-TSF being used by the Composite-ST without a new examination.

7 Having undertaken these steps the developer completes the preliminary Security Target for the composite product.

8 It is not mandatory that the platform and the composite TOE are being certified according to same version of the CC. It is due to the fact that the application can rely on some security services of the platform, if (i) the assurance level of the platform covers the intended assurance level of the composite TOE and (ii) the platform's security certificate is valid and up-to-date. Equivalence of single assurance components (and, hence, of assurance levels) belonging to different CC versions shall be established / acknowledged by the Composite Product Certification Body, cf. chapter 6.

9 If a PP conformance is claimed (e.g. composite ST claim conformance to a PP that claims conformance to a hardware PP), the consistency check can be reduced to the elements of the Security Target having not already been covered by these Protection Profiles.

The fact of compliance to a PP is not sufficient to avoid inconsistencies. Assume the following situation, where → stands for "complies with"

[9] because the TSF enforce the Security Target (together with organisational measures enforcing security objectives for the operational environment of the TOE).

[10] The comparison shall be performed on the abstraction level of SFRs. If the developer defined security functionality groups (TSF-groups) in the TSS part of his Security Target, the evaluator should also consider them in order to get a better understanding for the context of the security services offered by the TOE.

Composite-ST → SW PP → HW PP ← platform-ST

The SW PP may require any kind of conformance[11], but this does not change the 'additional elements' that the platform-ST may introduce to the HW PP. In conclusion, these additions are not necessarily consistent with the composite-ST/SW PP additions: There is no scenario that ensures the consistency 'by construction'.

Note that consistency may not be direct matching: e.g. objectives for the platform environment may become objectives for the composite TOE.

Dependencies:

10 No dependencies.

Developer action elements:

ASE_COMP.1.1D

11 The developer shall provide a statement of compatibility between the Composite Security Target and the Platform Security Target. This statement can be provided within the Composite Product Security Target.

Content and presentation of evidence elements:

ASE_COMP.1.1C

12 The statement of compatibility shall describe the separation of the Platform-TSF into relevant Platform-TSF being used by the Composite-ST and others.

ASE_COMP.1.2C

13 The statement of compatibility between the Composite Security Target and the Platform Security Target shall show (e.g. in form of a mapping) that the Security Targets of the composite product and of the underlying platform match, i.e. that there is no conflict between security environments, security objectives, and security requirements of the Composite Security Target and the Platform Security Target. It can be provided by indicating of the concerned elements directly in the Security Target for the composite product followed by explanatory text, if necessary.

Evaluator action elements:

ASE_COMP.1.1E

[11] e.g. "strict" or "demonstrable" according to CC V3.

14 The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Evaluator actions:

Action ASE_COMP.1.1E

ASE_COMP.1.1C

ASE_COMP.1-1 The evaluator shall check that the statement of compatibility describes the separation of the Platform-TSF into relevant Platform-TSF being used by the Composite-ST and others.

15 Please note that TSF means 'TOE Security Functionality' in CC V3, whereby the TSF content is represented by SFRs[12]. The respective TOE summary specification (TSS) shall provide, for each SFR, a description on how each SFR is met[13]. The evaluator shall use this description in order to understand the contextual frame of the SFRs.
If the developer defined security functionality groups (TSF-groups) in the TSS part of his Security Target as such contextual frame of the SFRs, the evaluator should also consider them in order to get a better understanding for the context of the security services offered by the TOE.

16 This work unit relates to the *Step 2* of the *Application Notes* above. In order to determine the intersection area the evaluator considers the list of the Platform-SFRs (given in the ST of the underlying platform) as single properties of the platform's security services.
To give an example, let us assume that there are the following Platform-SFRs: Cryptographic operations FCS_COP.1/RSA, FCS_COP.1/AES, FCS_COP.1/EC as well as tamper-resistance FPT_PHP.3 and limited capabilities and availability FMT_LIM.1 and FMT_LIM.2[14].

17 These Platform-SFRs shall be separated in three groups:

– **IP_SFR**: Irrelevant Platform-SFRs <u>not</u> being used by the Composite-ST.

– **RP_SFR-SERV:** Relevant Platform-SFRs being used by the Composite-ST to implement a security service with associated TSFI.

– **RP_SFR-MECH:** Relevant Platform-SFRs being used by the Composite-ST because of its security properties providing protection against attacks to the TOE as a whole and are

[12] security functional requirements

[13] cf. CC part 3, ASE_TSS.1.1C

[14] FMT_LIM.1 and FMT_LIM.2 can be found in PP-0084

addressed in ADV_ARC**.** These required security properties are a result of the security mechanisms and services that are implemented in the Platform TOE.

18 The second and third group *RP_SFR-SERV* and *RP_SFR-MECH* exactly represent the intersection area in question. For example, *IP_SFR* = {FCS_COP.1/AES}, *RP_SFR*-SERV= {FCS_COP.1/RSA, FCS_COP.1/EC } and *RP_SFR-MECH* = { FPT_PHP.3, FMT_LIM.1, FMT_LIM.2}, i.e. AES is not used by the composite TOE, but all other Platform-SFRs are used. However, the RP_SFR-MECH cannot be directly connected to SFRs in the Composite-ST.

19 The size of the overlapping area (i.e. the content of the group *RP_SFR-SERV* and *RP_SFR-MECH*) results from the concrete properties of the Platform-ST and the Composite-ST. If the Composite-ST does not use any property of the Platform-ST and, hence, the intersection area is an empty set (*RP_SFR-MECH* ∪ *RP_SFR-SERV*) = {∅}), no further composite evaluation activities are necessary at all: In such a case there is a technical, but not a security composition.

20 The result of this work unit shall be integrated to the result of ASE_REQ.1.6C/ ASE_REQ.1-10 (or the equivalent higher components if a higher assurance level is selected) and ASE_REQ.2.9C/ ASE_REQ.2-13.

ASE_COMP.1-2 The evaluator ***shall examine*** the statement of compatibility to determine that the Platform-TSF being used by the Composite-ST is complete and consistent for the current composite TOE.

21 In order to determine the completeness of the list of the Platform-TSF being used by the Composite-ST, the evaluator shall verify that:

– Platform-SFR = IP_SFR ∪ RP_SFR-SERV∪ RP-SFR-MECH

– Elements that belong to RP_SFR-SERV and RP-SFR-MECH are taken into account during the evaluation of the composite TOE. The IP-SFR are obviously part of the Platform-TOE but they are not considered during the evaluation of the composite TOE.

22 In order to determine the consistency of the list of the Platform-TSF being used by the Composite-ST, the evaluator shall verify that there are no ambiguities and contradictory statements.

23 More details on the consistency analysis can be found in common CC documents.

24 The result of this work unit shall be integrated to the result of ASE_REQ.1.6C/ ASE_REQ.1-10 (or the equivalent higher components if a higher assurance level is selected) and ASE_REQ.2.9C/ ASE_REQ.2-13.

ASE_COMP.1.2C

ASE_COMP.1-3 The evaluator ***shall check*** that the security assurance requirements of the composite evaluation represent a subset of the security assurance requirements of the underlying platform.

25 This work unit relates to the *Step 2* of the *Application Notes* above. In order to ensure a sufficient degree of trustworthiness of the Platform-TSF the evaluator compares the TOE security assurance requirements[15] of the composite evaluation with those of the underlying platform. The evaluator decides that the degree of trustworthiness of the Platform-TSF is sufficient, if the Composite-SAR represent a subset of the Platform-SAR:

$$\text{Platform-SAR} \supseteq \text{Composite-SAR},$$

e.g. the EAL chosen for the composite evaluation does not exceed the EAL applied to the evaluation of the platform.

26 The result of this work unit shall be integrated to the result of ASE_REQ.2.8C/ ASE_REQ.2-12.

ASE_COMP.1-4 The evaluator ***shall examine*** the statement of compatibility to determine that all performed operations on the relevant TOE security functional requirements of the platform are appropriate for the Composite-ST.

27 This work unit relates to *Step 3* of the *Application Notes* above. The *relevant* TOE security functional requirements of the platform comprise at least the elements of the group *RP_SFR-SERV* (cf. the work unit ASE_COMP.1-1) but also the *RP-SFR-MECH* may be presented as relevant TOE security functional requirements. The non-relevant TOE security functional requirements belong to IP_SFR.

28 In order to perform this work unit the evaluator compares single parameters of the *relevant* SFRs of the platform with those of the composite evaluation. For example, the evaluator compares the properties of the respective components FCS_COP.1/RSA and determines that the Composite-ST requires a key length of 2048 bit and the Platform-ST enforces the RSA-function with a

[15] denoted by SAR in the following

key length of 1024 and 2048 bit, i.e. this parameter of the platform is appropriate for the Composite-ST. Note, that the Composite-SFRs need not necessarily be the same as the Platform-SFRs, e.g. a trusted channel (FTP_ITC.1) in the composite product can be built using an RSA implementation (FCS_COP.1/RSA) of the platform.

29 The result of this work unit shall be integrated to the result of ASE_REQ.2.3C/ ASE_REQ.2-4.

ASE_COMP.1-5 The evaluator ***shall examine*** the statement of compatibility to determine that the relevant TOE security objectives of the Platform-ST are not contradictory to those of the Composite-ST.

30 This work unit relates to *Step 3* of the *Application Notes* above. The *relevant* TOE security objectives of the Platform-ST are those that are mapped to the *relevant* SFRs of the Platform-ST (cf. the work unit ASE_COMP.1-1).

31 In order to perform this work unit the evaluator compares the *relevant* TOE security objectives of the Platform-ST with those of the Composite-ST and determines whether they are not contradictory.

32 The result of this work unit shall be integrated to the result of ASE_OBJ.2.1C/ ASE_OBJ.2-1.

ASE_COMP.1-6 The evaluator ***shall examine*** the statement of compatibility to determine that the significant security objectives for the operational environments of the Platform-ST are not contradictory to those of the Composite-ST.

33 This work unit relates to *Step 3* of the *Application Notes* above. In order to determine which assumptions of the Platform-ST are *significant* for the Composite-ST the evaluator analyses the objectives for the environment of the Platform-ST and their separation in the following groups:

– **IrOE:** The objectives for the environment being not relevant for the Composite-ST, e.g. the objectives for the environment about the developing and manufacturing phases of the platform.

– **CfPOE**: The objectives for the environment being fulfilled by the Composite-ST *automatically*. Such objectives of the environment of the Platform-ST can always be assigned to the TOE security objectives of the Composite-ST. Due to this fact they will be fulfilled either by the Composite-SFR or by the Composite-SAR automatically. To give an example, let there be

an Objective for the environment OE.Resp-Appl of the Platform-ST: 'All User Data are owned by Smartcard Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as defined for the specific application context' and a TOE security objective OT.Key_Secrecy of the Composite-ST: 'The secrecy of the signature private key used for signature generation is reasonably assured against attacks with a high attack potential.' If the private key is the only sensitive data element, then the Objective for the environment OE.Resp-Appl is covered by the TOE security objective OT.Key_Secrecy automatically.

– **SgOE**: The remaining Objectives for the environment of the Platform-ST belonging neither to the group *IrOE* nor *CfOE* **Exactly this group makes up the *significant* objectives for the environment for the Composite-ST**, which shall be addressed in the Composite-ST.

34 In order to accomplish this work unit the evaluator compares the *significant* security objectives for the operational environment of the Platform-ST with those of the Composite-ST and determines whether they are not contradictory. If necessary, the *significant* security objectives for the operational environment of the Platform-ST shall be included into the Composite-ST including the related assumptions from which the objectives for the environment are drawn. The inclusion is not necessary, if the Composite-ST already contains equivalent (or similar) security objectives (covering all relevant aspects) and assumptions.

35 Since assurance of the development and manufacturing environment of the platform is confirmed by the platform certificate, the respective platform-objectives, if any, belong to the group *IrOE*

36 Assurance of development and manufacturing environment is usually completely addressed by the assurance class ALC, and, hence, requires no explicit security objective.

37 The result of this work unit shall be integrated to the result of ASE_OBJ.2.1C/ ASE_OBJ.2-1 and ASE_OBJ.2.3C/ ASE_OBJ.2-3.

Integration of composition parts and consistency check of delivery procedures (ALC_COMP)

The composite-specific work units defined in this chapter are intended to be integrated as refinements to the evaluation activities of the ALC class listed in the following table. The other activities of ALC class do not require composite-specific work units.

CC assurance family	Evaluation activity	Evaluation work unit	Composite-specific work unit
ALC_CMS	ALC_CMS.1.2C	ALC_CMS.1-2	ALC_COMP.1-1
AGD_PRE	AGD_PRE.1.1C	AGD_PRE.1-1	ALC_COMP.1-2
ALC_CMC	ALC_CMC.4.8C	ALC_CMC.4-10	ALC_CMC.4-10

NB: If the level of the assurance requirement chosen is higher than those identified in this table, the composite-specific work unit is also applicable.

ALC_COMP.1 Integration of the application into the underlying platform and Consistency check for delivery and acceptance procedures

Objectives

38 The aims of this activity are to determine whether

– the correct version of the application is installed onto/into the correct version of the underlying platform, and

– the preparative guidance procedures of **Platform** and **Application Developers** are compatible with the acceptance procedure of the **Composite Product Integrator**.

Dependencies:

39 No dependencies.

Developer action elements:

ALC_COMP.1.1D

40 The developer shall provide components configuration evidence; cf. item #7, item #8 and item #3 in Table 1, section 4.7.

41 .

Content and presentation of evidence elements:

ALC_COMP.1.1C

42 The components configuration evidence shall show that the evaluated version of the application has been installed onto / embedded into the certified version of the underlying platform

ALC_COMP.1.2C

43 The components configuration evidence shall show that:

(i) The evidence for delivery and acceptance compatibility shall show that the delivery procedures of the Platform and Application Developers are compatible with the acceptance procedure of the Composite Product Integrator.

(ii) the evidence shall show that preparative guidance procedures prescribed by the Platform and Application Developers are either actually being used by the Composite Product Integrator or compatible with the Composite Product Integrator guidance and do not contradict each other

Evaluator action elements:

ALC_COMP.1.1E

44 The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_COMP.1.2E

45 The evaluator shall confirm that the evidence for delivery compatibility is complete, coherent, and internally consistent.

Evaluator actions:

Action ALC_COMP.1.1E

ALC_COMP.1-1 The evaluator ***shall examine*** the evidence that the evaluated version of the application has been installed onto / embedded into the correct, certified version of the underlying platform.

46 The AGD_PRE documentation of the platform provided by the platform developer contains requirements for the secure acceptance of the platform and security measures to which the application developer or product composite integrator has to adhere. The application developer has to provide evidence that (if applicable), these requirements are followed up and the required security measures are implemented.

47 The *special* composite evaluator activity is to check the evidence of the version correctness for both parts of the composite product and that the secure acceptance and installation of the platform has been performed.

48 For the underlying platform, the evaluator shall determine that the actual identification of the platform is commensurate with the respective data in the platform certificate as part of following up on the procedures as specified in the AGD_PRE of the platform.

49 For the application, the relevant task is trivial due to the fact that the **Composite Product Evaluator** has to perform this task in the context of the assurance family ALC_CMS.

50 Components identification evidence can be supplied in two different ways: *technical* and *organisational*. A technical evidence of version correctness is being generated by the composite product itself: the platform and the application return – in each case – strings containing unambiguous version numbers as answers to the respective commands. E.g. it can be the return string of a command or the hard copy of the Windows-Information (like 'About'); in case of smart cards it can be an appropriate ATR.

51 A technical evidence of version correctness for hardware can also be supplied, if applicable, by reading off the unambiguous inscription on its surface. Note that there are no physical indication existing on most smart cards microcontrollers.

52 Technical evidence is recommended to be provided.

53 An organisational evidence of version correctness is being generated by the **Composite Product Integrator** on the basis of his configuration lists containing unambiguous version information of the platform and the application having been composed into the final composite product.

54 For example, in case of smart cards it can be an acknowledgement statement (e.g. configuration list) of the integrated circuit[16] manufacturer to the embedded software[17] manufacturer containing the evidence for the versions of the chip, the embedded software and its pre-personalisation parameters[18].

55 Organisational evidence is always possible and, hence, shall be provided.

56 The result of this work unit shall be integrated to the result of ALC_CMS1.1C/ ALC_CMS.1-2 (or the equivalent higher components if a higher assurance level is selected).

[16] -> underlying platform

[17] -> application

[18] Any data supplied by the embedded software manufacturer that is injected into the non-volatile memory by the integrated circuits manufacturer. These data are for instance used for traceability and/or to secure shipment between phases (cf. [Smartcard IC Platform Protection Profile with augmentation packages, Version 1.0, January 2014, registration number BSI-PP-084-2014], sec. 7.7).

ALC_COMP.1-2 The evaluator ***shall examine*** the acceptance procedure of the Composite Product Integrator, the delivery procedures of the Application Developer and the Platform developer to see that they are compatible and where necessary either applied by the Composite Product Integrator or prescribed in the preparative guidance. .

57 The *general* information of the preparative guidance requirements that amongst others includes configuration parameters is represented and has to be examined in the context of the assurance family AGD_PRE [1.2C]. The *special* evaluator activity is to examine the developer's evidence and to decide whether the **Composite Product Integrator** appropriately treats this *special subset* of the preparative guidance requirements.

58 The evaluator has to examine this provided evidence which includes the check whether the delivery procedures of the Platform and Application Developers are compatible with the acceptance procedure of the Composite Product Integrator.

59 In the cases where the **Composite Product Integrator** leaves preparative guidance requirements prescribed by the **Platform Developer** and **Application Developer** to the user, the **Composite Evaluator** verifies that such requirements are presented in the preparative guidance of the Composite evaluation.

60 For example, for a Java Card as Composite TOE, the Card Issuer has to set all parameters as prescribed by the Java Card Platform and the Applet Developers while installing the applet onto the Java Card platform; cf. Table 3, section 4.7. And And also verify that the package is byte code verified and has a valid digital signature.

61 The result of this work unit shall be integrated to the result of AGD_PRE.1.2C/AGD_PRE.1-4 and ALC_CMC.4.8C/ ALC_CMC.4-10

Composite design compliance (ADV_COMP)

The composite-specific work units defined in this chapter are intended to be integrated as refinements to the evaluation activities of the ADV class listed in the following table. The other activities of ADV class do not require composite-specific work units.

CC assurance family	Evaluation activity	Evaluation work unit	Composite-specific work unit
ADV_ARC	ADV_ARC.1.1E	ADV_ARC.1.1C/ ADV_ARC.1-1	ADV_COMP.1-1

ADV_IMP	ADV_IMP.1.1E	ADV_IMP.1.1C/ ADV_IMP.1-1	ADV_COMP.1-1
ADV_TDS	ADV_TDS.1.2E	ADV_TDS.1-7	ADV_COMP.1-1

NB: If the level of the assurance requirement chosen is higher than those identified in this table, the composite-specific work unit is also applicable.

ADV_COMP.1 Design compliance with the platform certification report, guidance and ETR_COMP

Objectives

62 The aim of this activity is to determine whether the requirements on the application, imposed by the underlying platform, are fulfilled in the composite product.

Application notes

63 The requirements on the application, imposed by the underlying platform, can be formulated in the relevant certification report (e.g. in form of constraints and recommendations), user guidance and ETR_COMP (in form of observations and recommendations) for the platform. The developer of the composite product shall regard each of these sources, if available (cf. Table 2, section 4.7), and implement the composite product in such a way that the applicable requirements are fulfilled.

64 The TSF of the composite product is represented at various levels of abstraction in the families of the development class ADV. Experiential, the appropriate levels of design representation for examining, whether the requirements of the platform are fulfilled by the composite product, are the TOE design (ADV_TDS), security architecture (ADV_ARC) and the implementation (ADV_IMP). In case, these design representation levels are not available (e.g. due to the assurance package chosen is EAL1), the current activity is not applicable (see the next paragraph for the reason).

65 Due to the definition of the composite TOE (cf. section 2.1 ‘Definitions’) the interface between the underlying platform and the application is the *internal* one, hence, a functional specification (ADV_FSP) as representation level is not appropriate for analysing the design compliance.

66 Security architecture ADV_ARC as assurance family is dedicated to ensure that integrative security services like domain separation, self-protection and non-bypassability properly work. It is impossible and not the sense of the composite evaluation to have an insight into the architectural internals of the underlying

platform (it is a matter of the platform evaluation). What the **Composite Evaluator** has to do in the context of ADV_ARC is

(i) to determine whether the application uses services of the underlying platform **within its own Composite-ST** to provide domain separation, self-protection, non-bypassability and protected start-up; if no, there is no further composite activities for ADV_ARC; if yes, then
(ii) the evaluator has to determine, whether the application uses these platform-services in an appropriate/secure way (please refer to the platform user guidance, cf. item #3 in Table 1, section 4.7).

67 Since consistency of the composite product security policy has already been considered in the context of the Security Target in the assurance family ASE_COMP (see page 31 above), there is no necessity to consider non-contradictoriness of the security policy model (ADV_SPM) of the composite TOE and the security policy model of the underlying platform.

Dependencies:

68 No dependencies.

Developer action elements:

ADV_COMP.1.1D

69 The developer shall provide a design compliance justification; cf. item #6 as well as items #3, #4, #5 in Table 1, section 4.7.

Content and presentation of evidence elements:

ADV_COMP.1.1C

70 The design compliance justification shall provide a rationale for design compliance – on an appropriate representation level – of how the requirements on the application, imposed by the underlying platform, are fulfilled in the composite product.

Evaluator action elements:

ADV_COMP.1.1E

71 The evaluator shall confirm that the rationale for design compliance is complete, coherent, and internally consistent.

Evaluator actions:

Action ADV_COMP.1.1E

ADV_COMP.1-1 The evaluator ***shall examine*** the rationale for design compliance to determine that all applicable requirements on the application, imposed by the underlying platform, are fulfilled by the composite product.

72 In order to perform this work unit the evaluator shall use the rationale for design compliance as well as the TSF representation

on the ADV_TDS, ADV_ARC and ADV_IMP levels on the one side and the input of the platform developer in form of the certification report, guidance and ETR_COMP on the other side. The evaluator shall analyse which platform requirements are applicable for the current composite product, based on the identified RP-SFR-MECH and RP-SFR-SERV. The evaluator shall compare each of the applicable requirements with the actual specification and/or implementation of the composite product and determine, for each requirement, whether it is fulfilled. As result, the evaluator confirms or disproves the rationale for design compliance.

73 For example, platform guidance may require the application to perform a special start-up sequence testing the current state of the platform and initialising its self-protection mechanisms. Such information might be found in the description of secure architecture ADV_ARC of the composite TOE; see also the *Application Note* above.

74 A second example, platform guidance may require the application to perform a DFA check on the DES operation, while the application is implementing BAC in an e-passport MRTD [PP-0055]. The ADV_ARC will explain whether the platform guidance is followed up or not, and in case that the requirements in the platform guidance are not followed a corresponding reasoning will be provided. The arguments of the developer explain why a non-compliancy will not introduce vulnerabilities.

75 The appropriate representation level (ADV_TDS, ADV_ARC and/or ADV_IMP), what the analysis is being performed on, can be chosen and mixed flexibly depending on the concrete composite TOE and the requirement in question. Where it is not self-explaining, the evaluator shall justify why the representation level chosen is appropriate.

76 The evaluator activities in the context of this work unit can be spread over different single evaluation aspects (e.g. over ADV_TDS and ADV_IMP). In this case the evaluator performs the partial activity in the context of the corresponding single evaluation aspect. Then the notation for this work unit shall be ADV_COMP.1-1-TDS, ADV_COMP.1-1-ARC and ADV_COMP.1-1-IMP, respectively.

77 If the assurance package chosen does not contain the families ADV_TDS, ADV_ARC or ADV_IMP (e.g. EAL1), this work unit is not applicable (cf. *Application Note* above).

78 The result of this work unit shall be integrated to the result of ADV_TDS.1−2E/ ADV_TDS.1-7, ADV_ARC.1.1E/

ADV_ARC.1.1C/ ADV_ARC.1-1, ADV_IMP.1.1E/ ADV_IMP.1.1C/ ADV_IMP.1-1 (or the equivalent higher components if a higher assurance level is selected).

Composite functional testing (ATE_COMP)

The composite-specific work units defined in this chapter are intended to be integrated as refinements to the evaluation activities of the ATE class listed in the following table. The other activities of ATE class do not require composite-specific work units.

CC assurance family	Evaluation activity	Evaluation work unit	Composite-specific work unit
ATE_COV	ATE_COV.1.1C	ATE_COV.1-1	ATE_COMP.1-1
ATE_FUN	ATE_FUN.1.2C	ATE_FUN.1-3	ATE_COMP.1-1

NB: If the level of the assurance requirement chosen is higher than those identified in this table, the composite-specific work unit is also applicable.

ATE_COMP.1 Composite product functional testing

Objectives

79 The aim of this activity is to determine whether composite product *as a whole* exhibits the properties necessary to satisfy the functional requirements of its Security Target.

Application notes

80 A composite product can be tested *separately* and *integrative*. Separate testing means that the platform and the application are being tested independent of each other. A lot of tests of the platform may have been performed within the scope of its accomplished evaluation. The application may be tested on a simulator or an emulator, which represent a virtual machine.
Integration testing means that the composite product is being tested as it is: the application is running on the platform.

81 Behaviour of implementation of some SFRs can depend on properties of the underlying platform as well as of the application (e.g. correctness of the measures of the composite product to withstand a side channel attack or correctness of the implementation of tamper resistance against physical attacks). In such a case the SFR implementation shall be tested on the final composite product, but not on a simulator or an emulator.

82 This activity focuses exclusively on testing of the composite product *as a whole* and represents merely *partial efforts* within the general test approach being covered by the assurance ATE. These integration tests shall be specified and performed, whereby

the approach of the standard[19] assurance families of the class ATE shall be applied.

83 - A correct behaviour of the Platform-TSF being relevant for the Composite-ST (corresponding to the group *RP_SFR-SERV* and *RP-SFR-MECH* in the work unit ADV_COMP.1-1 above),and-absence of exploitable vulnerabilities (sufficient effectiveness) in the context of the Platform-ST are confirmed by the valid Platform Certificate, cf. chapter 6 above.

Dependencies:

84 No dependencies.

Developer action elements:

ATE_COMP.1.1D

85 The developer shall provide a set of tests as required by the assurance package chosen.

ATE_COMP.1.2D

86 The developer shall provide the composite TOE for testing.

Content and presentation of evidence elements:

ATE_COMP.1.1C

87 Content and presentation of the specification and documentation of the *integration* tests shall correspond to the standard[20] requirements of the assurance families ATE_FUN and ATE_COV.

ATE_COMP.1.2C

88 The composite TOE provided shall be suitable for testing.

Evaluator action elements:

ATE_COMP.1.1E

89 The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Evaluator actions:

Action ATE_COMP.1.1E

[19] i.e. as defined by CEM

[20] i.e. as defined by CEM

ATE_COMP.1-1 The evaluator ***shall examine*** that the developer performed the *integration* tests for all SFRs having to be tested on the composite product as a whole.

90 In order to perform this work unit the evaluator shall analyse, for each SFR, whether it directly depends on security properties of the platform and of the application. Then the evaluator shall verify that the *integration* tests performed by the developer cover at least all such SFRs.

91 If the assurance package chosen does not contain the families ATE_FUN and ATE_COV (e.g. EAL1), this work unit is not applicable.

92 The result of this work unit shall be integrated to the result of ATE_COV.1−1C/ ATE_COV.1-1 and ATE_FUN.1.2C/ ATE_FUN.1-3 (or the equivalent higher components if a higher assurance level is selected).

Composite vulnerability assessment (AVA_COMP)

The composite-specific work units defined in this chapter are intended to be integrated as refinements to the evaluation activities of the AVA class listed in the following table. The other activities of AVA class do not require composite-specific work units.

CC assurance family	Evaluation activity	Evaluation work unit	Composite-specific work unit
AVA_VAN	AVA_VAN.1.3E	AVA_VAN.1-5	AVA_COMP.1-1
	AVA_VAN.1.3E.	AVA_VAN.1-6	AVA_COMP.1-2
	AVA_VAN.1.3E	AVA_VAN.1-7	AVA_COMP.1-2
	AVA_VAN.1.3E	AVA_VAN.1-8	AVA_COMP.1-2

NB: If the level of the assurance requirement chosen is higher than those identified in this table, the composite-specific work unit is also applicable.

AVA_COMP.1 Composite product vulnerability assessment

Objectives

93 The aim of this activity is to determine the exploitability of flaws or weaknesses in the composite TOE *as a whole* in the intended environment.

Application notes

94 This activity focuses exclusively on vulnerability assessment of the composite product *as a whole* and represents merely *partial*

efforts within the general approach being covered by the standard[21] assurance family of the class AVA: AVA_VAN.

95 The results of the vulnerability assessment for the underlying platform represented in the ETR_COMP can be reused under the following conditions: they are up to date and all composite activities for correctness – ASE_COMP.1, ALC_COMP.1, ADV_COMP.1 and ATE_COMP.1 – are finalised with the verdict PASS.

96 Due to composing of the platform and the application a new quality arises, which can cause additional vulnerabilities of the platform which might be not mentioned in the ETR_COMP. In these circumstances [R44] applies.

Dependencies:

97 No dependencies.

Developer action elements:

AVA_COMP.1.1D

98 The developer shall provide the composite TOE for penetrating testing.

Content and presentation of evidence elements:

AVA_COMP.1.1C

99 The composite TOE provided shall be suitable for testing *as a whole*.

Evaluator action elements:

AVA_COMP.1.1E

100 The evaluator shall conduct penetration testing of the composite product *as a whole* building on evaluator's own vulnerability analysis, to ensure that the vulnerabilities being relevant for the Composite-ST are not exploitable.

Evaluator actions:

Action AVA_COMP.1.1E

AVA_COMP.1-1 The evaluator ***shall examine*** the results of the vulnerability assessment for the underlying platform to determine that they can be reused for the composite evaluation.

[21] i.e. as defined by CEM

101 The results of the vulnerability assessment for the underlying platform are usually represented in the ETR_COMP. They can be reused if the following conditions are met: they are up to date and all composite activities for correctness – ASE_COMP.1, ALC_COMP.1, ADV_COMP.1 and ATE_COMP.1 – are finalised with the verdict PASS. The evaluator shall also consider the relevant determinations in the Platform Certification Report. For validity of the platform security certificate please refer to chapter 6 above. It is noted that the platform itself could be a composite TOE. This means also that the validity of each ETR for composition of the TOEs that compose the platform TOE must be checked.

102 When the validity of the ETRs for composition is checked, the necessity of checking the contents depends on the application and user available TSFI. If the TSFI are available to the user or used by the application, the content of the ETR must be checked. If not and formal platform TSFI are no longer available as TSFI, the validity date of the ETR_COMP is sufficient.

103 The result of this work unit shall be integrated to the result of AVA_VAN.1.3E/ AVA_VAN.1-5 (or the equivalent higher components if a higher assurance level is selected).

AVA_COMP.1-2 The evaluator ***shall specify, conduct and document*** penetration testing of the composite product *as a whole*, using the standard approach of the assurance family AVA_VAN.

104 If the correctness-related activities – ASE_COMP.1, ALC_COMP.1, ADV_COMP.1 and ATE_COMP.1 – are finalised with the verdict PASS and the certificate for the platform covers all security properties needed for the composite product, composing of the platform and the application must not create additional vulnerabilities of the platform.

105 If the evaluator determined that composing of the platform and the application creates additional vulnerabilities of the platform[22], a contradiction to the verdict PASS for the correctness activities (see paragraph 95 above) has to be supposed or the certificate for the platform does not cover all security properties needed for the current composite product.

106 The result of this work unit shall be integrated to the result of AVA_VAN.1.3E/ AVA_VAN.1-6, AVA_VAN.1-7, AVA_VAN.1-8 (or the equivalent higher components if a higher assurance level is selected).

[22] i.e. not mentioned in the ETR_COMP

Appendix 2: ETR for composite evaluation template

The related document "JIL-ETR-template-for-composition" shall be used as a template by the **Platform Developer** to issue the ETR_COMP. Please note that the layout can be customized according to the evaluation facilities company standard, but the contents and structure are mandatory.

Appendix 3: Platform user guidance examples

Disclaimer: This section is not meant to be an appendix of an actual ETR for Composite evaluation but is included to support the platform developer in creation of user guidance requirements. These user guidance requirements have to be implemented by the embedded software developer in the application to protect the TOE against certain attacks.

User guidance requirements that are provided to the application developer must have the following properties:

1. It must be clear what the user has to do to protect the TOE
2. It must be clear for which attack (path or partial attack) the requirement is protecting from. The detail must be such that an embedded software developer will be able to perform a design compliance analysis. In other words, if a certain attack is not relevant for an application the formulation must be such that an application developer will recognise this.